

# THE DEPARTMENT OF DEFENSE INFORMATION TECHNOLOGY SECURITY CERTIFICATION AND ACCREDITATION PROCESS (DITSCAP)<sup>1</sup>

**Jack Eller**

DISA, CISS (ISBEC)  
701 South Courthouse Rd.  
Arlington, VA 22204-4507

**Mike Mastrorocco**

Computer Security Consulting  
107 Windsor Drive  
Mineral Wells, WV 26150

**Barry C. Stauffer**

CORBETT Technologies, Inc.  
228 N. Saint Asaph St.  
Alexandria, VA 22314

## Abstract

On August 19, 1992 the Office of Assistant Secretary of Defense directed the Defense Information Systems Agency (DISA) Center for Information Systems Security (CISS) to formulate a standard DoD process for security certification and accreditation. CISS formed a working group, consisting of Service and Agency representatives. The working group evaluated ten existing processes, but found none which could be adopted Department of Defense (DoD)-wide. As a result, the working group developed the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) [1]. A standard process across DoD, DITSCAP applies to accreditation of both strategic and tactical systems, as well as stand-alone information systems or networks. DITSCAP capitalized on approved security techniques, software, and procedures to reduce the complexity and overall cost of the accreditation process. The DITSCAP integrates security directly into the system life cycle and is designed so that it can be applied uniformly across DoD. The DITSCAP defines a process which standardizes all activities leading to a successful accreditation, thereby minimizing the risks associated with nonstandard security implementations across shared Defense Information Infrastructure (DII) and end systems. The DITSCAP has been designed to support the requirements of Office of Management and Budget Circular A-130 [2].

In contrast to the prevailing system based accreditation processes, the DITSCAP is focused on the infrastructure and views systems and networks as components of the infrastructure. The view of the DITSCAP, therefore, differs from such documents as the National Computer Security Center (NCSC) Certification and Accreditation Process Handbook for Certifiers (NCSC-TG-031) [3]. CISS and the NCSC have agreed that for the near term, NCSC-TG-031 provides sound guidelines. DITSCAP provides the midterm and long term infrastructure-centric approach to the security certification and accreditation of systems and networks. These two processes have been harmonized to reflect the transition to the DITSCAP. Both terminology and structural parallels will facilitate a smooth transition between these two processes.

## 1. Introduction

The DITSCAP establishes a standardized process, set of activities, general task descriptions, and a management structure to verify, validate, implement and maintain the security posture of the DII. The DITSCAP is designed to be adaptable to any type of Information Technology (IT) and any computing environment and mission. It can be adapted to include existing system certifications and evaluated products. It can use new security technology or programs, and adjust to the appropriate standards. The process may be aligned with any program acquisition strategy. Its activities can be integrated into the system life cycle to ensure the system meets

---

<sup>1</sup> The DITSCAP was developed for CISS under Logicon, Inc. Contract DAAB07-91-D-B519

the accreditation requirements during development and integration and continues to maintain the accredited security posture after fielding. While DITSCAP maps to any system life cycle

process, its four phases are independent of the life cycle strategy. The DITSCAP's, four phases, Figure 1, are: Definition, Verification, Validation, and Post Accreditation. Phase I, **Definition**, focuses on understanding the mission, environment, and architecture to determine the security requirements and level of effort necessary to achieve accreditation. Phase II, **Verification**, verifies the evolving, or modified, system's compliance with the agreed upon security requirements. Phase III, **Validation**, validates the fully integrated system's compliance with the security requirements. Phase III concludes with full approval to operate the system, e.g., security accreditation. Phases I, II, and III are the DITSCAP process engine. The DITSCAP methodology permits the forward or backward movement between phases to keep pace with the system development or to resolve problems. Therefore the phases are repeated as often as necessary to produce an accredited system. The objective of Phase IV, **Post Accreditation**, is to ensure system management, operation, and maintenance to preserve an acceptable level of residual risk. Phase IV includes those activities necessary for the continuing operation of the accredited system.

Each phase is performed for every system and every process activity within each phase is performed. However, the procedures within each process activity may be tailored and scaled to the system and its associated acceptable level of residual risk. The procedures are a set of established tasks which can be tailored to fit the mission, environment, system architecture, and programmatic considerations. These procedures consist of planning, certification, development, maintenance, operation, change management, and compliance validation actions. In this manner, the process maintains flexibility to deal with different acquisition strategies, situations, and operational scenarios.

## **2. Phase I Definition**

Phase I activities focus on definition of the certification and accreditation task. This is the planning phase which documents all results in the System Security Authorization Agreement (SSAA). Phase I is similar to other certification and accreditation processes in that the planning is begun, appropriate security officials are identified, responsibilities are assigned, data is collected and a security plan is initiated. Unlike other processes, Phase I ends with a formal agreement of the definition of the architecture and boundaries of the system to be certified, security requirements, certification approach, work plan, and level of effort. Phase I is not completed until this agreement is reached. Phase I is revisited throughout the process, whenever necessary, to update this agreement.

The key to the DITSCAP is the agreement which is reached in Phase I between the IT system Program Manager, the Designated Approving Authority (DAA), and the User Representative. These three managers resolve critical schedule, budget, security, availability, functionality, and performance issues and document that agreement in the SSAA.

Phase I contains three process activities; Mission Need, Registration, and Negotiation. The input to phase I includes all available system documentation, security requirements, system requirements, and the Concept Of Operations. The output from Phase I is the SSAA. The three process activities provide the pathway to understanding the system; documenting the security requirements; developing a security architecture; and determining the scope, level of effort, documentation required, and schedule for the planning and certification actions. Phase I begins with analyzing or developing the mission need. The mission need is either a document or compilation of information which state the systems requirements and intended capabilities. It

includes the definition of the system mission, functions and interfaces; organization(s) to operate the system; the intended operational environment; information types and classifications; expected system life cycle; system user characteristics; and intended interfaces with other systems or networks. As implied by the process activity name (mission need), the DITSCAP starts as soon as the concept for a system is developed. If the system of interest is an existing system, the process starts when a security relevant modification is being planned, or upon the periodic reaccreditation.

Registration starts the dialogue between the Program Manager, the DAA, and the Users of the system. The Program Manager and the DAA appointed Certification Authority work together to perform the certification actions. During Registration, information is collected and evaluated, applicable security requirements are determined, risk management and vulnerability assessment activities begin, and the level of effort required for certification and accreditation is determined and planned. Registration begins with a review of the mission need and concludes with preparation of an initial draft of the SSAA. These activities involve the collection of necessary information to determine security requirements and the level of effort to accomplish the certification and accreditation commensurate with the level of assurance required for confidentiality, integrity, availability, and accountability. The results of the Registration activities are documented in the SSAA. The draft SSAA is then submitted to the Program Manager, DAA, and User Representative for their review. The tasks required during Registration activities include:

- Prepare a high level system description including system boundaries and interfaces.
- Determine the system program acquisition strategy and life cycle of the system.
- Assess the impact of the system life cycle phase on the certification effort.
- Determine the classification and types of information to be processed.
- Determine the clearances and access requirements of the processes and users.
- Identify the system class and develop the system security requirements.
- Identify the organizations that will support the DITSCAP.
- Tailor the DITSCAP activities.
- Determine the scope, level of effort and schedule for the DITSCAP activities.

Negotiation is the activity where all the participants involved in the information system's development, acquisition, operation, security certification, and accreditation agree upon the implementation strategy to be used to satisfy the security requirements identified during system registration. The key parties who must reach agreement during the negotiations are the Program Manager, the DAA, and the User Representative. Negotiation is NOT a bargaining session to determine which requirements to implement and which to delete. The purpose of negotiation is to ensure that all participants understand their roles and responsibilities and that the SSAA properly and clearly defines the requirements, the approach, and the level of activity. Negotiation concludes with the approval of the SSAA by the Program Manager, DAA, and User Representative.

The SSAA documents the conditions of certification and accreditation for an IT system. The SSAA is used throughout the entire DITSCAP to guide activities, document decisions, specify security requirements, document certification tailoring and level-of-effort, identify potential solutions, and maintain operational systems security. The SSAA is a "living", master document intended to reduce the need for repetitive documents by consolidation of all security related information into one document. The SSAA is the baseline reference for future decisions. As such it is particularly helpful during personnel changes and program budget modifications.

### **3. Phase II Verification**

The activities of Phase II, verify the system's compliance with the requirements agreed on in the SSAA. Phase II activities include continuing refinement of the SSAA, system development or modification, and certification analysis. Phase II starts with a review and, if necessary, refinement of the SSAA. At each stage of the development or modification, the SSAA is refined by adding details to reflect the current state of the system. As the development or modification progresses and specific information relating to the certification effort becomes available, the SSAA is updated to include more specific details. As details about the hardware and software architecture become available, this information is added to the SSAA to support the agreed upon level of certification actions. Since the Program Manager, DAA, and User Representative concur with all changes of the SSAA, they are continually appraised on the security requirements, DITSCAP activities, and level-of-effort. As a result there are no surprises at certification and accreditation time.

The life cycle activities in Phase II are those activities required to develop and integrate the system components. Each life cycle activity has a corresponding Phase II certification analysis activity. These certification activities verify by analysis, investigation, and comparison that the IT design implements the SSAA requirements and the security critical components function properly. Certification analysis compliments the functional testing which occurs during Phase III. While every system may be considered certifiable, the DITSCAP goal is to produce systems that satisfy operational requirements with an acceptable level of risk. The DITSCAP analysis actions, therefore, are performed in step with the system development to ensure the development, modification, and integration efforts will result in a certifiable and accreditable information system, before Phase III begins. In this manner, DITSCAP becomes a success oriented process.

Six<sup>2</sup> certification actions or tasks are performed during Phase II. These include:

- System Architecture analysis verifies that the system architecture complies with the architecture description agreed upon in the SSAA.
- Software Design analysis evaluates how well the software implements the security requirements of the SSAA and the security architecture of the system.
- Network Connection Rule Compliance analysis evaluates connections to other systems and networks to ensure the system design will enforce security policies.
- Product integrity analysis evaluates the integration of non-developmental software, hardware, and firmware to ensure their integration complies with the system security architecture, and the integrity of each product is maintained.
- Life Cycle Management analysis verifies that change control and configuration management practices are, or will be, in place and are sufficient.

---

<sup>2</sup>The 21 INFOSEC analysis tasks described in the "Certification and Accreditation Process Handbook for Certifiers", NCSC-TG-031, have been restructured into 14 tasks in the DITSCAP.

- Vulnerability Assessment evaluates security vulnerabilities and recommends appropriate countermeasures.

At the completion of the Phase II Certification Analysis, the system will have a documented security specification, a comprehensive test plan, and assurance that all network and other interconnections requirements have been implemented. A vulnerability assessment will have been conducted and will have concluded that the infrastructure needs of the system, e.g., configuration management, will be accommodated throughout the system life cycle.

At the conclusion of each life cycle development milestone, the certification analysis results are reviewed for SSAA compliance. Should the results indicate significant deviation from the SSAA, the DITSCAP reverts to Phase I to resolve the problems. If the results are acceptable, the DITSCAP proceeds to the next development activity or to government acceptance and security testing, i.e., DITSCAP Phase III. Upon completion of certification analysis, the system proceeds to Phase III, which contains the formal system certification test and security accreditation actions.

#### **4. Phase III Validation**

Phase III activities, Figure 1, validate that preceding work has produced a system that operates in a specified computing environment with an acceptable level of residual risk. Phase III begins with a review of the SSAA to ensure that its requirements and the agreements are current. The SSAA review is followed by an evaluation of the IT system, certification, and accreditation. Phase III activities occur after the system is integrated and culminate in system accreditation.

Certification Evaluation includes eight actions to certify that the fully integrated system is ready for operational deployment. These actions include:

- System Security Testing and Evaluation to assess the technical and nontechnical implementation of the security features and their proper performance.
- Penetration Testing, for appropriate system classes, to assess the system's ability to withstand attempts to circumvent system security features.
- TEMPEST and Red/Black Verification to validate that the equipment and site meet the applicable TEMPEST security requirements.
- Validation of COMSEC Compliance to ensure that COMSEC approval has been granted and approved COMSEC key management procedures are used.
- System Management Analysis to examine the management infrastructure to determine if it will maintain the mission, environment, and architecture described in the SSAA.
- Site Accreditation Surveys to validate that the operational procedures for the IT, environmental concerns, and physical security pose no unacceptable risks.
- Contingency Plan examination to verify that the contingency and continuity of service plans are consistent with the SSAA.

- Risk Management Review to assess the operation of the system to determine if the risk is being maintained at an acceptable level.

At the conclusion of Phase III, the certifier prepares a recommendation to the DAA. The recommendation, supporting documentation, and the SSAA form the accreditation package. The supporting documentation should include security findings, deficiencies, risks of operation and all information necessary to support the recommended decision. After the accreditation decision is made, the system now progresses to Phase IV.

## **5. Phase IV Post Accreditation**

Phase IV contains activities necessary to operate and manage the system so that it will maintain an acceptable level of residual risk. Post-accreditation activities include; ongoing maintenance of the SSAA, system operations, change management, and compliance validation. Phase IV begins after the system has been integrated into the operational computing environment and accredited. Phase IV continues until the information system is removed from service. As in the preceding phases, the SSAA must be kept current.

The second Phase IV activity, Operation, concerns the secure operation of the system and the associated computing environment. System maintenance activities ensure the system continues to operate within the stated parameters of the accreditation. These activities identify changes in hardware, software, and system design. The system security officer determines the extent to which a change affects the security posture of either the information system or the computing environment. Changes that significantly affect the system security posture must be forwarded to the DAA, User Representative, and Program Manager. In this manner, the system continues to operate under Phase IV while the proposed changes are considered under Phase I of the DITSCAP. The three managers then decide what certification and accreditation actions are required in response to the proposed change.

Compliance Validation is a periodic review of the operational system and its computing environment to ensure the continued compliance with the security requirements, current threat assessment, and concept of operations as stated and agreed upon in the SSAA.

## **6. Process Management Roles and Responsibilities**

The management approach for DITSCAP focuses on systems level management to execute DITSCAP. The management concept integrates existing roles into the certification and accreditation process to provide visibility into the process to all managers responsible for system development, operation, maintenance, security, and to system users.

There are three key roles in the DITSCAP, the system Program Manager, the DAA, and the User Representative. These three managers cooperate to provide the most capable system with an acceptable (tolerable) level of risk. They develop and approve the security requirements, manage the certification and accreditation process, and review the results. They must reach agreement during Phase I "Negotiation" and approve the SSAA. During Phases II, III, and IV, if the system is changed, or any of the agreements delineated in the SSAA are modified, the three key parties return to Phase I Negotiation and revise the SSAA as

necessary. The DITSCAP allows these three managers to tailor and scope the certification and accreditation efforts to the particular mission, environment, system architecture, threats, funding, schedule, and criticality of the system.

## **7. Summary**

The DITSCAP provides the common framework to certify and accredit all DoD IT systems within the network infrastructures they employ and to maintain the security of these systems throughout their life cycle. While the activities in the four DITSCAP phases are mandatory, the implementation details may be tailored to meet the need of the particular system.

Potential savings are anticipated for all organizations involved in DoD certification and accreditation. Reuse of security architectures, designs, or certification evidence is facilitated by categorizing systems into a set of system classes. The SSAA consolidates and reduces documentation requirements eliminating the repetition of information in multiple documents. The use of the standard process should eliminate duplicate efforts and promote common acceptance of data generated by different agencies and DAAs. The use of system classes facilitates the sharing of results.

## References

- [1] Department of Defense (DoD) Information Technology Security Certification and Accreditation Process (DITSCAP), July 1996.
- [2] Office of Management and Budget (OMB) Appendix III to OMB Circular No. A-130 - Security of Federal Automated Information Resources, February 1996.
- [3] National Computer Security Center (NCSC) Certification and Accreditation Process Handbook for Certifiers (NCSC-TG-031), July 1996.